UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/859,429	05/18/2001	Makoto Kayashima	566.39530VX1	5340

24956 7590 05/08/2006

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314

EXAMINER	
KHOSHNOODI, NADIA	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/859,429	KAYASHIMA ET AL.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *8-13* is/are pending in the application.

4a) Of the above claim(s) *1-7* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *8-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 May 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 09/761,742.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/30/2006 has been entered.

Response to Amendment

Applicant's arguments/amendments with respect to amended claims 8-13 filed 1/30/2006 have been fully considered (See 37 CFR 1.111; MPEP 714.04) but they are not persuasive.

Response to Arguments

Applicant contends that Wiegel and Grimm et al. fail to teach or suggest the described features of the present invention regarding the providing of "security control means and means for obtaining the status and changing the configuration of the security control means in the appropriate manner relative to security specifications." Examiner respectfully disagrees. Grimm et al. teach a security policy service that includes various security controls which allow one to obtain the status, as well as to change the configuration of the security control means (col. 5, lines 13-51). Therefore, Grimm et al. do teach the described features of the present invention regarding the providing of security control means and means for obtaining the status and changing the configuration of the security control means in the appropriate manner relative to

security specifications. Furthermore, one would have been motivated to modify Wiegel in order to allow for the limitation of "obtaining the status and changing the configuration of the security control means in the appropriate manner relative to security specifications" because Grimm et al. suggest that it is important to evaluate each system's security policy to ensure that they are diagnosed and managed properly in order to ensure system security (col. 5, lines 13-51).

Applicants then generally state that the cited prior arts of record do not teach or suggest "the security specification hatching step, the security diagnosing step and the security handling and management step" (i.e. the entire claim). Below, Examiner has presented the specific portions of each of the cited prior arts of record relied upon as teaching each specifically claimed limitation.

Applicant contends that Wiegel fails to teach or suggest "a security hatching step of executing an information security policy which corresponds to each managed system constituting an information system designated by a user from a database describing a correspondence between information security policies representing policies of security measures with at least one managed system and the managed systems, to hatch security specification to be applied to the information system" as recited in the claims. Examiner respectfully disagrees.

Wiegel substantially teaches the claimed security management method for supporting a security management of each of a plurality of managed systems constituting an information system with an electronic computer, comprising a security specification hatching step of extracting an information security policy made to correspond to each managed system constituting an information system (col. 13, lines 29-37 and fig. 7B, elements 726, 728, and 730) designated by a user (col. 13, lines 38-49) from a database (col. 11, lines 43-47 and col. 14, lines

20-35) describing a correspondence of the information security policy (col. 13, lines 38-49) representing policies of a security measure with at least one managed system (col. 13, lines 1-9 and 49-56), to hatch security specifications (col. 13, lines 14-20) to be applied to the information system (col. 13, lines 20-22).

Applicant also contends that Wiegel also fails to teach or suggest "a security diagnosis step of executing a plurality of audit programs describing a processing for auditing various information including a type of the managed and a software version, which are stored so as to correspond to each set of the information security policy and the managed system which are specified by the hatched security specifications as well as by a security status to audit the various information including the type of the software version of the managed system constituting the information system designated by the user and diagnose a security of the information system" as recited in the claims. Examiner agrees that Wiegel does not explicitly disclosed these claimed features, however, Examiner respectfully disagrees with the statement that Grim et al. fail to teach or suggest these features of the present invention. Grimm et al. teach a security diagnosis step of executing a plurality of audit programs (fig. 1, elements 11 and 21) describing a process for auditing various information (col. 7, lines 27-34), including a type of the managed system (col. 4, lines 9-34) and a software version (col. 5, lines 16-27), stored so as to correspond to each set of the information security policy and the managed system (col. 5, lines 39-59) which are specified by security specifications hatched in said security specification hatching step (as applied with Wiegel above), as well as by a security status to audit the various information including the type and the software version of the managed system (col. 7, lines 27-34)

constituting the information system designated by the user (fig. 2, element 10), and to diagnose a security of said information system (fig. 2, element 14 and col. 5, lines 13-39).

Furthermore, Applicant also contends that Wiegel fails to teach or suggest "a security handling and management step of executing a management program designated by the user from a plurality of management programs describing a process for controlling the security status concerning the security policy of the managed system stored so as to correspond to each set of the information security policy and the managed system which are specified by the hatched security specifications to allow the electronic computer to change the security status of the managed system corresponding to the management program so as to adjust the security status to the information security policy corresponding to the management program" as recited in the claims. Examiner agrees that Wiegel does not explicitly disclosed these claimed features, however, Examiner respectfully disagrees with the statement that Grim et al. fail to teach or suggest these features of the present invention. Grimm et al. teach a security handling and management step of executing a management program designated by the user, from a plurality of management programs (col. 4, lines 24-34 and fig. 1, element 17) describing a process for controlling the security status concerning the information security policy of the managed system, stored so as to correspond to each set of the information security policy and the managed system (col. 5, lines 39-59) which are specified by the security specifications hatched in said security specification hatching step (as applied with Wiegel above), to allow said electronic computer to change the security status of the managed system (col. 4, lines 35-61) corresponding to the management program so as to adjust the security status to the information security policy that corresponds to the management program (col. 5, lines 52-63).

Due to the reasons stated above, the Examiner maintains rejections with respect to amended claims 8-13. Grim et al. in combination with Wiegel teach the limitations not explicitly disclosed by Wiegel. Therefore, it is the Examiner's conclusion that amended claims 8-13 are not patentably distinct or non-obvious over the prior art of record as presented.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 8-11 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegel United States Patent No. 6,484,261 and further in view of Grimm et al. United States Patent No. 6,317,868.

As per claim 8:

Wiegel substantially teaches the claimed security management method for supporting a security management of each of a plurality of managed systems constituting an information system with an electronic computer, comprising a security specification hatching step of extracting an information security policy made to correspond to each managed system constituting an information system (col. 13, lines 29-37 and fig. 7B, elements 726, 728, and 730) designated by a user (col. 13, lines 38-49) from a database (col. 11, lines 43-47 and col. 14, lines 20-35) describing a correspondence of the information security policy (col. 13, lines 38-49) representing a policy of a security measure with at least one managed system (col. 13, lines 1-9

and 49-56), to hatch security specifications (col. 13, lines 14-20) to be applied to the information system (col. 13, lines 20-22).

Not explicitly disclosed by Wiegel is a security diagnosis step of executing a plurality of audit programs describing a process for auditing various information, including a type of the managed system and a software version, stored so as to correspond to each set of the information security policy and the managed system which are specified by security specifications hatched in said security specification hatching step, as well as by a security status to audit the various information including the type and the software version of the managed system constituting the information system designated by the user, and to diagnose a security of said information system; and a security handling and management step of executing a management program designated by the user, from a plurality of management programs describing a process for controlling the security status concerning the information security policy of the managed system, stored so as to correspond to each set of the information security policy and the managed system which are specified by the security specifications hatched in said security specification hatching step, to allow said electronic computer to change the security status of the managed system corresponding to the management program so as to adjust the security status to the information security policy that corresponds to the management program.

However, Grimm et al. teach a security diagnosis step of executing a plurality of audit programs (fig. 1, elements 11 and 21) describing a process for auditing various information (col. 7, lines 27-34), including a type of the managed system (col. 4, lines 9-34) and a software version (col. 5, lines 16-27), stored so as to correspond to each set of the information security policy and the managed system (col. 5, lines 39-59) which are specified by security

specifications hatched in said security specification hatching step (as applied with Wiegel above), as well as by a security status to audit the various information including the type and the software version of the managed system (col. 7, lines 27-34) constituting the information system designated by the user (fig. 2, element 10), and to diagnose a security of said information system (fig. 2, element 14 and col. 5, lines 13-39).

Also disclosed by Grimm et al. is a security handling and management step of executing a management program designated by the user, from a plurality of management programs (col. 4, lines 24-34 and fig. 1, element 17) describing a process for controlling the security status concerning the information security policy of the managed system, stored so as to correspond to each set of the information security policy and the managed system (col. 5, lines 39-59) which are specified by the security specifications hatched in said security specification hatching step (as applied with Wiegel above), to allow said electronic computer to change the security status of the managed system (col. 4, lines 35-61) corresponding to the management program so as to adjust the security status to the information security policy that corresponds to the management program (col. 5, lines 52-63).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the method disclosed in Wiegel to add a security diagnosis step and a security handling/management step as disclosed by Grimm et al. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so as suggested by Grimm et al. in "enforcing and auditing site-specific security provisions" (col. 1, lines 15-18 and col. 1, line 58 – col. 2, line 29).

As per claim 9:

Wiegel and Grimm et al. substantially teach the security management method as applied to claim 8 above. Furthermore, Grimm et al. substantially teach the method wherein in said security diagnosis step, the audit program made to correspond to each set of the information security policy and the managed system, which are specified by the security specifications hatched in said security specification hatching step, is extracted (col. 5, lines 13-51) describing a correspondence of the information security policy, the managed system and the audit program describing a processing for auditing various information such as a type and a software version of said managed system as well as the security status concerning said information security policy of said managed system, and executed, to diagnose the security of the information system designated by said user.

Also, Grimm et al. substantially teach in said security handling and management step, the management programs made to correspond to each set of the information security policy and the managed system, which are specified by the security specifications hatched in said security specification hatching step, are extracted (col. 4, lines 24-34) describing a correspondence of the information security policy, the managed system and the management program describing a processing for controlling the security status concerning the security policy, the managed system and said information security policy of a security of said managed system, and the management program designated by the user is extracted among the extracted programs to be executed (col. 4, lines 24-44), to allow the security status of the managed system corresponding to the extracted management program to adjust to the information security policy corresponding to the management program.

Not explicitly disclosed by Wiegel or Grimm et al. are the audit program and the management programs being extracted from a database. However, Wiegel teaches the method wherein the audit program and the management programs, which are used for configuring and maintaining the system, are extracted from a database. Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the method disclosed in Wiegel and Grimm et al. to allow for the audit program and management programs to be extracted from the database. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Wiegel suggests it is important to have the ability to extract audit records in order to properly manage the system in col. 11, lines 43-51.

As per claim 10:

Wiegel and Grimm et al. substantially teach the security management method as applied in claim 8 above. Not explicitly disclosed by Wiegel or Grimm et al. is the method wherein said security diagnose step is executed periodically. However, Grimm et al. teaches the method wherein said security diagnose step is executed periodically as defined by the user. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Grimm et al. to allow for the security diagnose step to be executed periodically. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Grimm et al. suggest that periodically executing the diagnose step will make the system as a whole more secure in col. 5, lines 42-51.

As per claim 11:

Wiegel and Grimm et al. substantially teach the security management method as applied to claim 8. Not explicitly disclosed by Wiegel or Grimm et al. is that method wherein, in accordance with setting a content received from the user, said management program changes the security status of the managed system corresponding to the management program so as to adjust the security status to the information security policy corresponding to the management program. However, Wiegel teaches a security setting content received from the user. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wiegel and Grimm et al. to incorporate a security setting content received from the user in order for the management program to change the security status of the managed system. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Wiegel suggests that it is important for the management program to adjust the security settings of the system based on any security instances that arise in order to maintain the most up-to-date secure system as possible in col. 14, lines 1-61.

As per claim 13:

Wiegel substantially teaches the claimed security management system for supporting a security management of managed systems constituting an information system, comprising a database (col. 11, lines 43-47 and col. 14, lines 20-35) describing a correspondence of an information security policy (col.13, lines 38-49) representing a policy of a security measure with at least one managed system (col. 13, lines 1-9 and 49-56) and a security specification hatching section for extracting an information security policy made to correspond to each of the managed systems constituting the information system (col. 13, lines 29-37 and fig. 7B, elements 726, 728,

and 730) designated by a user (col. 13, lines 38-49) from said database (col. 11, lines 43-47 and col. 14, lines 20-35), to hatch security specifications (col. 13, lines 14-20) to be applied to the information system (col. 13, lines 20-22).

Not explicitly disclosed by Wiegel is a plurality of audit sections for auditing various information including a type and a software version of the managed system as well as a security status concerning the information security policy of the managed system, each audit section being provided so as to correspond to each set of the information security policy and the managed system, which are specified by security specifications hatched by said security specification hatching section, a security diagnosis section for diagnosing a security of an information system designated by said user, on the basis of diagnosis results in each of said audit sections, a plurality of management sections for controlling a security status concerning the information security policy of the managed system, each management section being provided so as to correspond to each set of the information security policy and the managed system, which are specified by security specifications hatched by said security specification hatching step, and a security handling and management section for executing a management section designated by said user, to change the security status of the managed system corresponding to the management program so as to adjust the security status to the information security policy corresponding to the management program.

However, Grimm et al. teach a security management system for supporting a security management of managed systems constituting an information system comprising a plurality of audit sections (fig. 1, elements 11 and 21) for auditing various information (col. 7, lines 27-34), including a type (col. 4, lines 9-34) and a software version of the managed system (col. 5, lines

16-27), as well as a security status concerning the information security policy of the managed system (col. 7, lines 27-34), each audit section being provided so as to correspond to each set of the information security policy and the managed system (col. 7, lines 27-34), which are specified by security specifications hatched by said security specification hatching section (as applied with Wiegel above) and a security diagnosis section for diagnosing a security of an information system designated by said user (fig. 2, element 10), on the basis of diagnosis results in each of said audit sections (col. 5, lines 13-39 and fig. 2, element 14).

Also disclosed by Grimm et al. is a plurality of management sections (col. 4, lines 24-34 and fig. 1, element 17) for controlling a security status concerning the information security policy of the managed system, each management section being provided so as to correspond to each set of the information security policy and the managed system (col. 5, lines 39-59) which are specified by security specifications hatched in said security specification hatching step (as applied with Wiegel above) and a security handling and management section for executing a management section designated by said user (col. 4, lines 24-34 and fig. 1, element 17), to change the security status of the managed system (col. 4, lines 35-61) corresponding to the management program so as to adjust the security status to the information security policy corresponding to the management program (col. 5, lines 52-63).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the method disclosed in Wiegel to add a security diagnosis step and a security handling/management step as disclosed by Grimm et al. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so as suggested by Grimm et al.

in "enforcing and auditing site-specific security provisions" (col. 1, lines 15-18 and col. 1, line 58 – col. 2, line 29).

III. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wiegel United States Patent No. 6,484,261, Grimm et al. United States Patent No. 6,317,868, and further in view of CERT's CC Vendor-Initiated Bulletins 1994-1998.

As per claim 12:

Wiegel and Grimm et al. substantially teach the security management method, wherein a diagnosis results obtained in said security diagnose step which is executed for the information system designated by the user are reflected in the database describing the correspondence of the information security policy with at least one managed system and an audit/management program stored so as to correspond to each set of the information security policy and the managed system as applied to claim 8 above. Not explicitly disclosed by Wiegel or Grimm et al. is security hole information published by a security information organization including CERT or Computer Emergency Response Team. However, CERT/CC Vendor–Initiated Bulletins disclose security hole information published by a security information organization including CERT. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wiegel and Grimm et al. to incorporate the use of security hole information published by a security information organization including CERT or Computer Emergency Response Team. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since CERT/CC Vendor –Initiated Bulletins 1994-1998 suggest that it is very important to deal with security vulnerabilities as soon as possible which means that it is necessary to report

vulnerabilities as discovered in order to allow all users to take the necessary precautions in pages 1-8.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nadia Khoshnoodi
Examiner
Art Unit 2137
5/3/2006

NK

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER